REMARKS/ARGUMENTS

Favorable consideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-22 are pending in the application.

In the Official Action, Claims 1-22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Caronni (U.S. Patent No. 6,507,908) in view of Inoue et al. (U.S. Patent No. 6,170,057, hereinafter Inoue).

Briefly recapitulating, Claim 1 is directed to a gateway device for carrying out a data relaying at a transport or upper layer between a first terminal device and a second terminal device which are capable of carrying out communication through networks with data secrecy based on a security association set up therebetween. The gateway device includes a security information management unit configured to obtain and manage information regarding the security association. The gateway device also includes a data receiving unit configured to receive encrypted data from the first terminal device or the second terminal device. The gateway device also includes a data decryption unit configured to obtain decrypted data by decrypting the encrypted data by using the information regarding the security association at a time of relaying the communications with data secrecy between the first terminal device and the second terminal device. The gateway device also includes a data relay unit configured to carry out the data relaying at the transport or upper layer according to the decrypted data. The gateway device also includes a data encryption unit configured to encrypt data to be transmitted from the gateway device by using the information regarding the security association. The gateway device also includes a data transmitting unit configured to transmit the encrypted data by the data encryption unit to the second terminal device or the first terminal device, respectively.

2

As described in Applicants' specification, the object of the present invention is to effectively combine a method for providing security such as IPSec and a device, such as a TCP-GW, and a Snoop proxy particularly provided between wired side terminal devices and wireless side terminal devices, for improving performance of TCP. Thus, the gateway according to the present invention is located between a first terminal device and a second terminal device. The first and second terminal devices are in security association with each other and thus carry out communications with each other with data secrecy based on the security association. The gateway obtains information regarding the security association from somewhere. This is because the gateway itself does not have a function to secure secret communications between the first device and the second device. The gateway of the present invention is provided as a proxy device for improving performance of TCP.

Thus, the gateway of Claims 1, 19 and 21 decrypts encrypted data received from the first terminal device or the second terminal device according to the information regarding the security association. Next, the gateway according to the present invention carries out a data relaying at a transport or upper layer according to the decrypted data. The gateway encrypts data to be transmitted, according to the information regarding the security association.

Caronni describes a method for secure data communications with a mobile machine in which a data packet is received from the mobile machine having a particular network address. A pool of secure addresses is established and a data structure is created to hold address translation associations. Each association is between a particular network address and a particular one of the secure addresses. If the receive data packet is a secure data packet an association between the received data packets network address and a secure address in the data structure is identified and the data packets network address is translated to the associated secure address before forwarding the data packet onto higher network protocol layers. When the received data packet is not secure it is passed on without address translation to the higher

network protocol layers. For outgoing packets addressed to a secure address, the secure

address is translated to a real network address and the packet payload is encrypted. Outgoing

packets that are addressed directly to the real network addresses passed through in a

conventional manner.[1]

However, as acknowledged in the Official Action, while Caronni decrypts data from

an external device, Caronni does not decrypt the data according to the information regarding

the security association.

Inoue describes a mobile computer and a packet encryption and an authentication

method which are capable of controlling an activation of a packet encryption and

authentication device belonging to the mobile computer according to the security policy at

the visited network of the mobile computer. The mobile computer is provided with a packet

encryption and authentication unit having an on/off switchable functional for applying an

encryption and authentication processing on input/output packets of the mobile computer.

One of the packet encryption authentication unit and an external packet processing device is

selectively controlled to carry out the encryption and authentication processing on the

input/output packets, where the external packet processing device being provided in a visited

network at which the mobile computer is located and having a function for relaying packets

transferred between a computer located in the network and a computer located in another

network by applying the encryption and authentication processing.[2]

However, contrary to the Official Action, like Caronni, Inoue fails to disclose or

suggest the feature that "a gateway re-encrypts the decrypted packets obtained from

decrypting the received packets before sending them to a destination device". That is, Inoue

fails to disclose or suggest a gateway that receives encrypted packets and then decrypts the

---

[1] Caronni Abstract.
[2] Inoue, Abstract.

4

encrypted packets and then re-encrypts the decrypted packets and then sends this encrypted packets.

Column 2, lines 42-49 in Inoue merely describes "gateway 4a (where the packet is decrypted) → home agent (HA) 4 → getaway 4a (where the packet is encrypted again)". Sending and receiving a packet between the decryption and encryption is quite different from decrypting a packet, using the decrypted packet and then re-encrypting the packet.

Column 5, lines 30-42 in Inoue merely describes that "the data routing control with respect to the mobile computer 2 is carried out by encapsulating an IP packet destined to an original address (an address in a home network la) of the mobile computer 2 within a packet destined to a current location address of the mobile computer 2". Furthermore, column 5, lines 43-50 in Inoue merely describes that "each gateway has a packet encryption and authentication processing function". Each of these portions of Inoue fail to disclose or suggest that a gateway re-encrypts the decrypted packets (obtained from decrypting the received packets) before sending them to a destination device.

Column 7, lines 55-65 in Inoue merely discloses that "the gateway 6 applies the encryption and authentication processing to both the packet that is received from the Internet 6 and is sent to the mobile station 2 and the packet that is received from the mobile station 2 and is sent to the Internet 6". This portion of Inoue also fails to disclose or suggest "a gateway re-encrypts the decrypted packets obtained from decrypting the received packets before sending them to a destination device".

Because Inoue fails to cure Caronni by disclosing or suggesting "a gateway re-encrypts the decrypted packets obtained from decrypting the received packets before sending them to a destination device," Applicants submit the outstanding rejection under 35 U.S.C. § 103(a) is improper.

Furthermore, Applicants continue to traverse the finding that <u>Caronni</u> describes a security association between first and second devices. That is, in <u>Caronni</u>, only an internal secure network is secured from an external terminal such as a mobile device. The gateway recited in Applicants' claims decrypts encrypted data received from the first terminal device or the second terminal device <u>according to the information regarding the security association</u>. In addition, the gateway recited in Applicants' independent claims relays data at a transport or upper layer <u>according to the decrypted data</u>. <u>Caronni</u> fails to disclose or suggest any data relaying operation, let alone Applicants' recited relay at a transport or upper layer <u>according to the decrypted data</u>. By relaying at a transport or upper layer <u>according to the decrypted data</u>, present invention is provided as a proxy device for improving performance of TCP, whereas the gateway in <u>Caronni</u> merely maintains access control lists (ACLs) to prevent unauthorized devices from accessing the secure network. Similarly, <u>Caronni</u> does not encrypt the data <u>according to the information regarding the security association</u>. <u>Inoue</u> fails to cure the deficiencies of <u>Caronni</u>.

Applicants' Claims 10, 20 and 22 recite an authentication function to attach authentication information to data to be transmitted to the second terminal device or the first terminal device <u>according to the information regarding the security association</u>. <u>Caronni</u> fails to disclose or suggest such an authentication operation. <u>Inoue</u> fails to cure the deficiencies of <u>Caronni</u>.

MPEP §706.02(j) notes that to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference disclosings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must disclose or suggest all the claim limitations. Also, the disclosing or

suggestion to make the claimed combination and the reasonable expectation of success must

both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d

488, 20 USPQ2d 1438 (Fed. Cir. 1991). Without addressing the first two prongs of the test

of obviousness, Applicants submit that the Official Action does not present a *prima facie* case

of obviousness because both <u>Caronni</u> and <u>Inoue</u> fail to disclose all the features of Applicants'

claimed invention.

Accordingly, in view of the present amendment and in light of the previous

discussion, Applicants respectfully submit that the present application is in condition for

allowance and respectfully request an early and favorable action that that effect.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Michael E. Monaco
Registration No. 52,041

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\MM\AMENDMENT\0039\208915US.AM DUE 10-27-05.DOC

7